Synapse Bootcamp - Module 3

Exploring and Filtering Data - Exercises

Objectives

In these exercises you will learn:

- How to use the Explore feature in Tabular display mode.
- How to use the `pivot` menu to pivot to connected nodes.
- How to use the `query` menu option to filter results.

Note: We are constantly updating Synapse and its Power-Ups! We do our best to make sure our course documents (slides, exercises, and answer keys) are up-to-date. However, you may notice small differences (such as between a screen capture in the documents and the appearance of your current instance of Synapse).

If something is unclear or if you identify an error, please reach out to us so we can assist!

Exercises

Navigating Data in Synapse

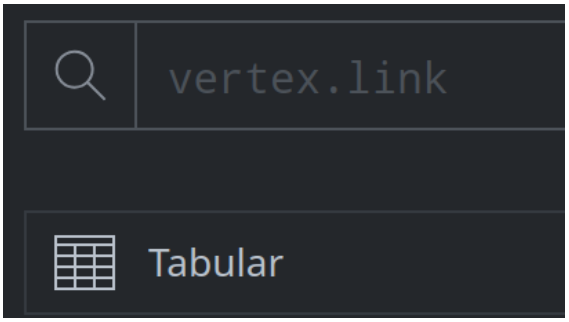
Exercise 1

Objective:
- **Use the Synapse Explore button to navigate and view data in Tabular display mode.**
- **Use the 'pivot' menu to navigate by specific connections in the data**

Part 1

View tags on a node to get information about the node.

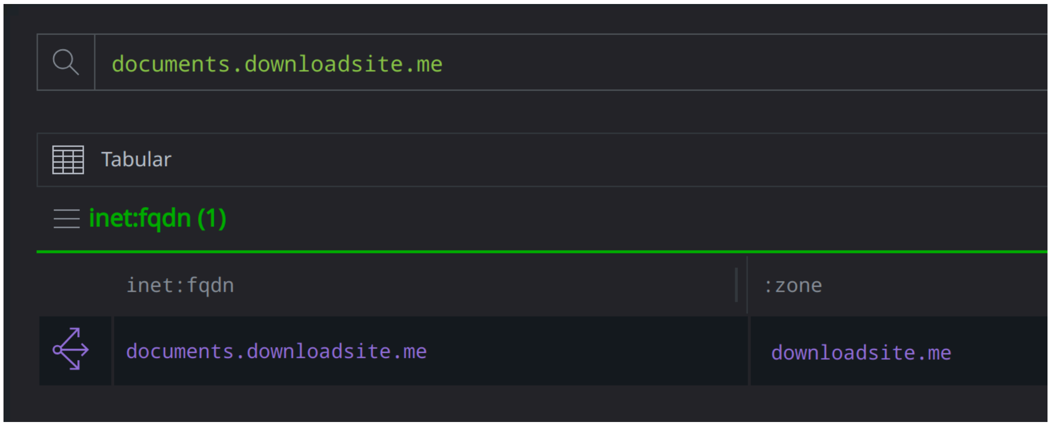
- In the **Research Tool,** ensure your **Storm Query Bar** is in **Lookup mode** and your display mode is set to **Tabular:**



- Enter the following in your **Query Bar** and press **Enter** to run the query:

```
documents.downloadsite.me
```

- **Select** the node in your **Results Panel:**

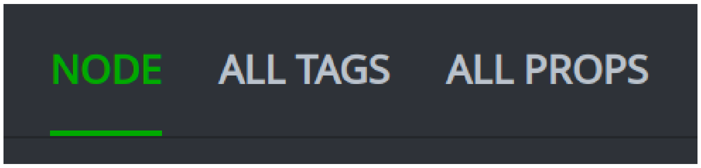


documents.downloadsite.me

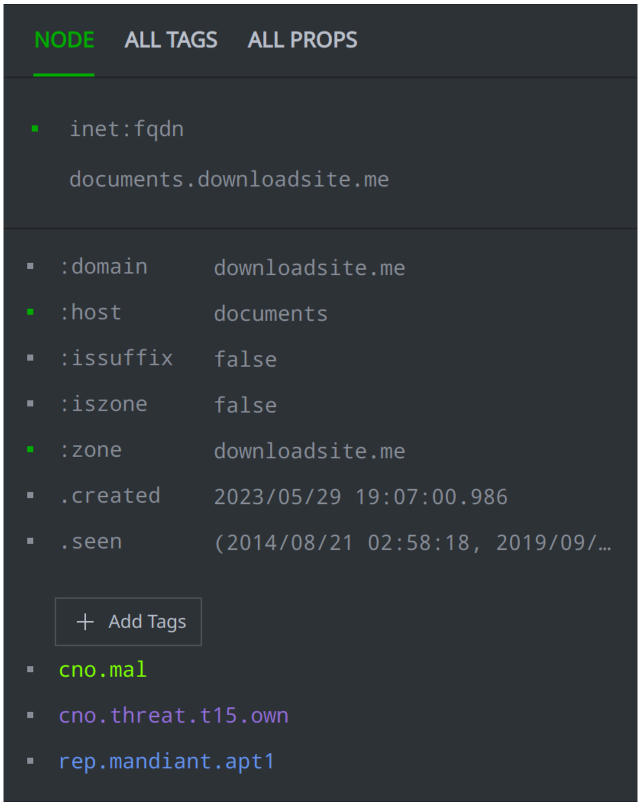
inet:fqdn (1)

inet:fqdn	:zone
documents.downloadsite.me	downloadsite.me

- In the **Details Panel,** select the **NODE** tab:



- View the **tags** on the node:



inet:fqdn

documents.downloadsite.me

:domain	downloadsite.me
:host	documents
:issuffix	false
:iszone	false
:zone	downloadsite.me
.created	2023/05/29 19:07:00.986
.seen	(2014/08/21 02:58:18, 2019/09/…

- cno.mal
- cno.threat.t15.own
- rep.mandiant.apt1

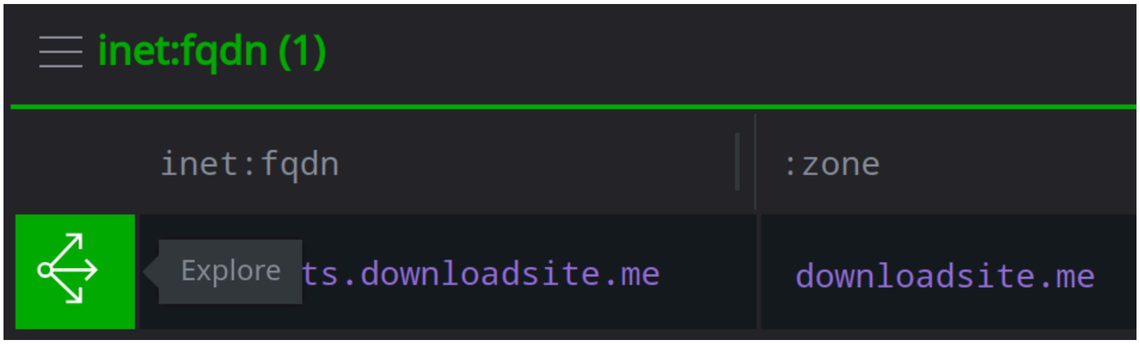
Question 1: What do the tags tell us about this FQDN?

Tip: If you do not know what a tag means, you can:

- **hover over** the tag to see its definition; or
- look up the tag in **Tag Explorer.**

See other nodes that this node is connected to in Synapse.

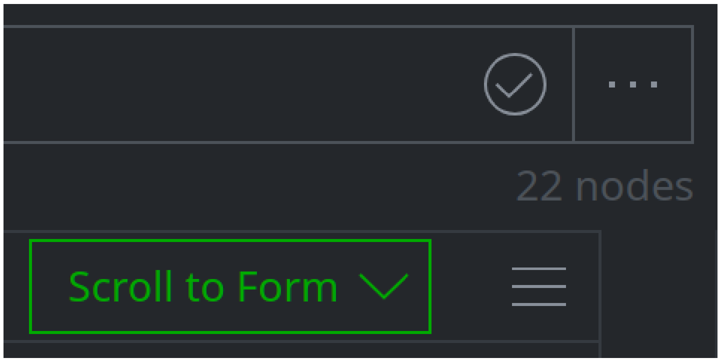
- Click the **Explore** button next to the FQDN to display adjacent nodes:



inet:fqdn (1)

inet:fqdn	:zone
ts.downloadsite.me	downloadsite.me

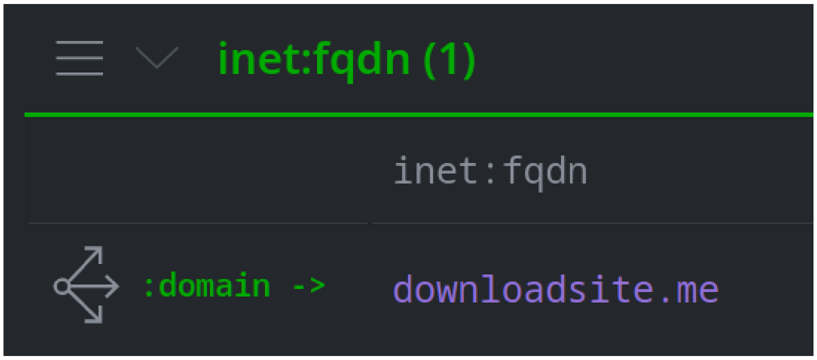
- Click the **Scroll to Form** button to view the kinds of nodes that are "connected" to the FQDN:



Question 2: What kinds of nodes are "connected" to the FQDN?

Use the **link column** to understand "how" nodes are connected.

- In your current set of results, locate the **inet:fqdn** node (use **Scroll to Form** if necessary):



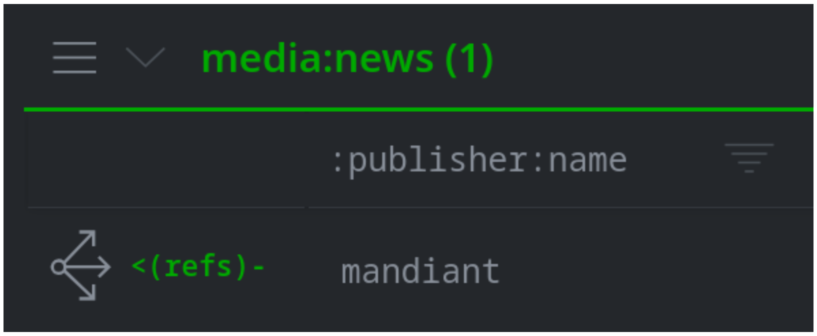
inet:fqdn (1)

	inet:fqdn
:domain ->	downloadsite.me

- Look at the value in the **link column.**

Question 3: How is the FQDN **`downloadsite.me`** connected to your original FQDN (`documents.downloadsite.me`)?

- In your current set of results, locate the **media:news** node (use **Scroll to Form** if necessary):



media:news (1)

	:publisher:name
<(refs)-	mandiant

- Look at the value in the **link column.**

Question 4: How is the **`media:news`** node connected to your original FQDN (`documents.downloadsite.me`)?

Part 2

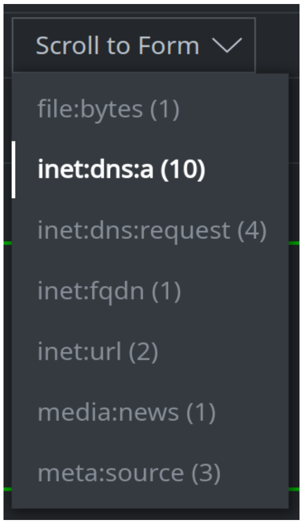
There are common questions we ask when we identify a malicious FQDN:

- "What IP addresses has this FQDN resolved to?"
    - This may help us identify attacker infrastructure.
- "Are there any files that query this FQDN?"
    - This may help us identify malware that connects to the FQDN.

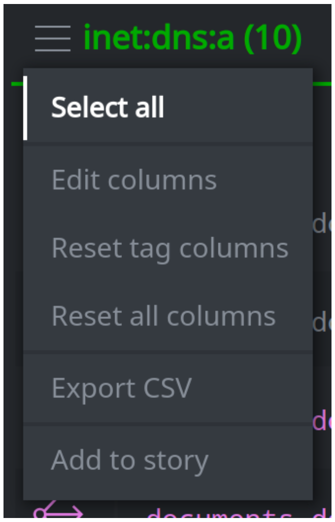
We will use Synapse's **Explore** button to answer these questions.

Search for attacker infrastructure by Exploring to DNS A records for `documents.downloadsite.me` and associated IPv4s.

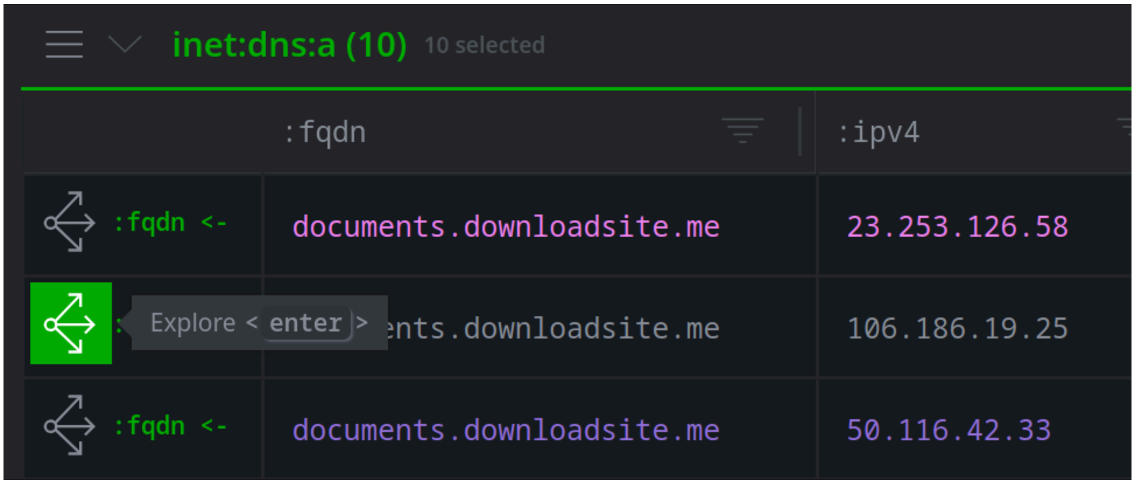
- Using your existing results, click the **Scroll to Form** button and select **inet:dns:a** from the dropdown list to view the connected DNS A records:



- Click the **hamburger menu** to the left of the **inet:dns:a** header and choose **Select all:**

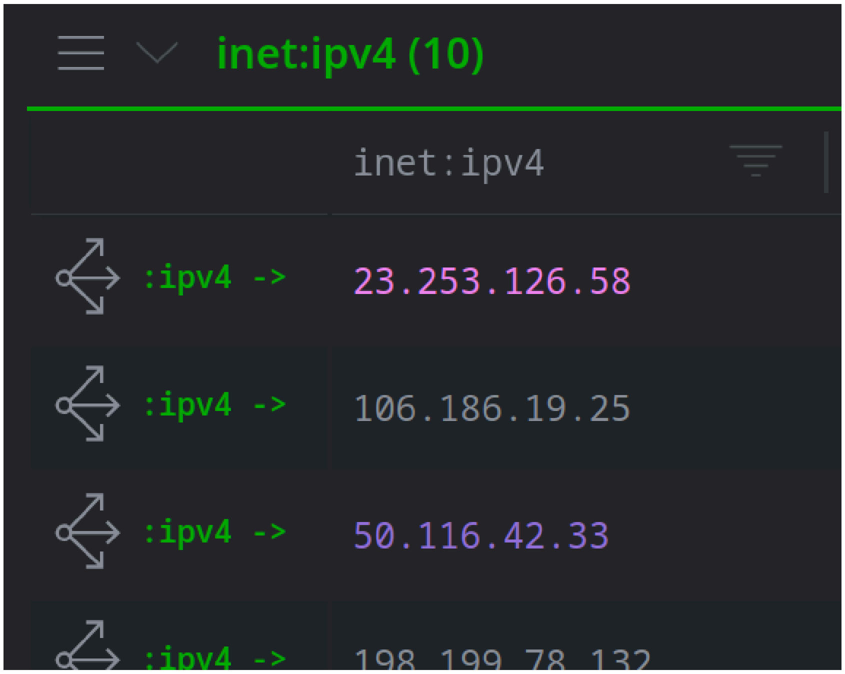


- Click the **Explore** button next to any of the selected **`inet:dns:a`** nodes to display adjacent nodes:



	:fqdn	:ipv4
:fqdn <-	documents.downloadsite.me	23.253.126.58
:	ents.downloadsite.me	106.186.19.25
:fqdn <-	documents.downloadsite.me	50.116.42.33

- Locate and view the **`inet:ipv4`** nodes in your results:



inet:ipv4 (10)

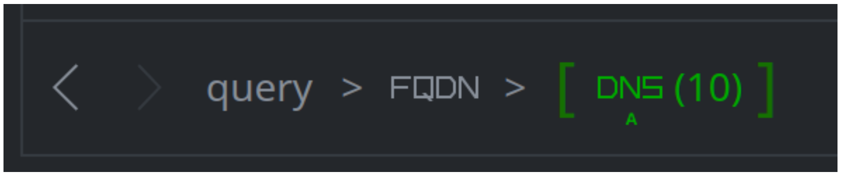
	inet:ipv4
:ipv4 ->	23.253.126.58
:ipv4 ->	106.186.19.25
:ipv4 ->	50.116.42.33
:ipv4 ->	198.199.78.132

Question 5: What information is available for the IP addresses, based on their **properties** and **tags?**

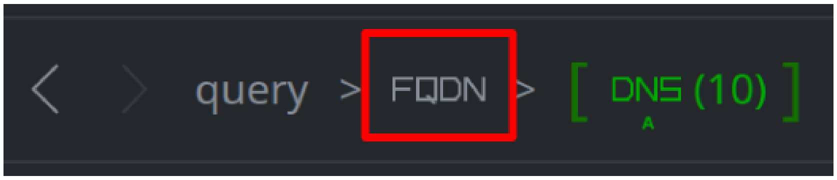
Part 3

Search for malware by Exploring to DNS requests and associated files.

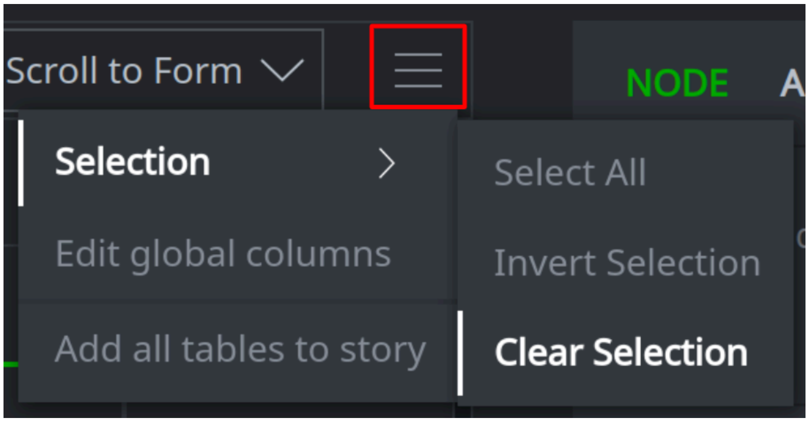
- In your current set of results, locate your **breadcrumbs:**



- Click **FQDN** to return to our previous **Explore** results:

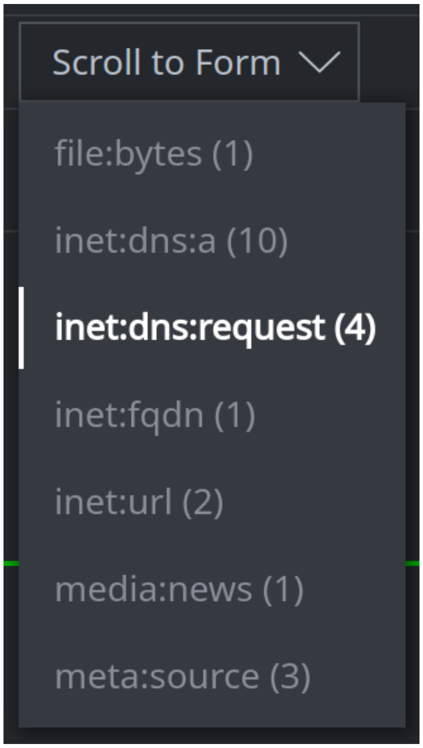


- The **`inet:dns:a`** nodes are currently **selected.** From the display mode **hamburger menu,** click **Selection > Clear Selection:**

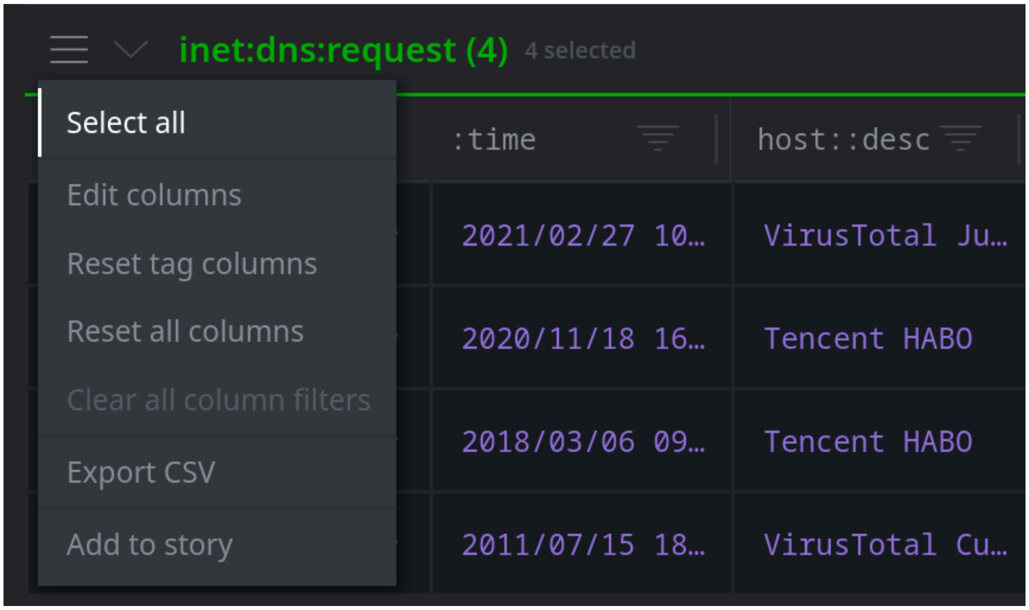


This will **deselect** the **`inet:dns:a`** nodes so we can Explore from other forms.

- Click the **Scroll to Form** button and select **inet:dns:request** from the dropdown list:

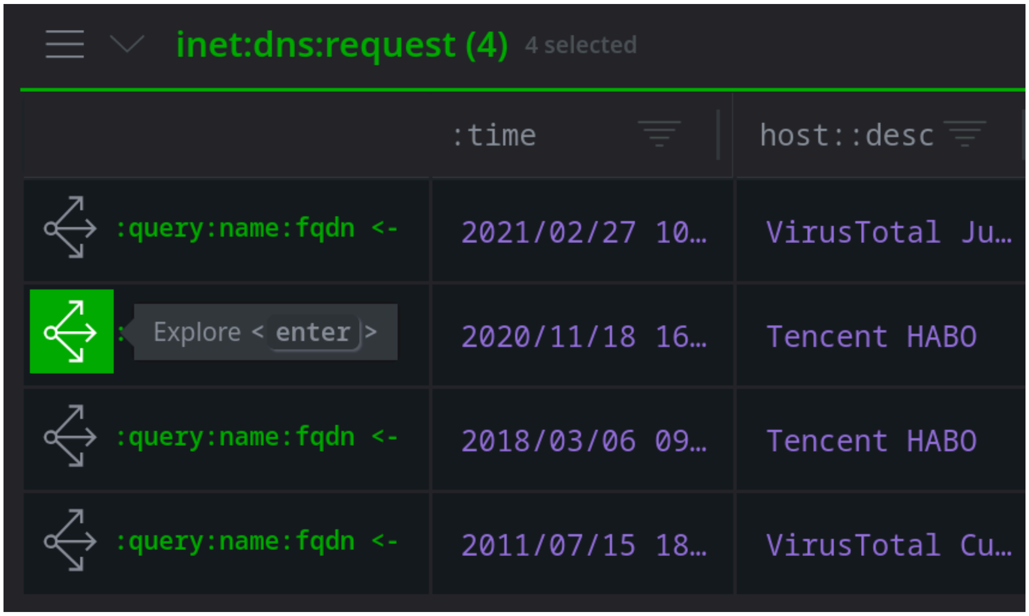


- Click the **hamburger menu** to the left of the **inet:dns:request** header and choose **Select All:**



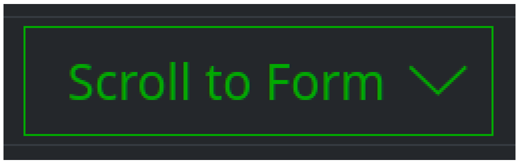
:time	host::desc
2021/02/27 10…	VirusTotal Ju…
2020/11/18 16…	Tencent HABO
2018/03/06 09…	Tencent HABO
2011/07/15 18…	VirusTotal Cu…

- Click the **Explore** button next to any selected `inet:dns:request` node to display adjacent nodes:



	:time	host::desc
:query:name:fqdn <-	2021/02/27 10…	VirusTotal Ju…
:	2020/11/18 16…	Tencent HABO
:query:name:fqdn <-	2018/03/06 09…	Tencent HABO
:query:name:fqdn <-	2011/07/15 18…	VirusTotal Cu…

- Locate the **`file:bytes`** nodes in your results (use **Scroll to Form** if necessary):

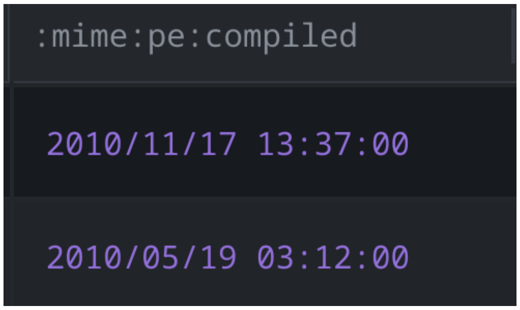


Question 6: How many files query the FQDN **`documents.downloadsite.me`**?

Part 4

Search for all files with the same compile time.

- From your current set of results, identify the file with a compile time of **2010/11/17 13:37:00**

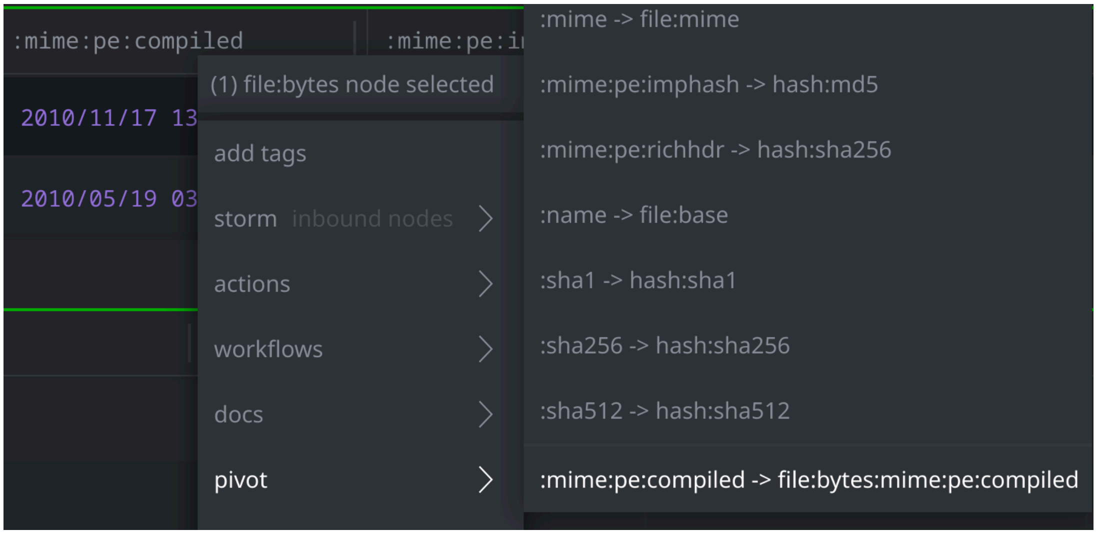


:mime:pe:compiled

2010/11/17 13:37:00

2010/05/19 03:12:00

- **Right-click** on that **`file:bytes`** node's **`:mime:pe:compiled`** property value, and select **pivot > :mime:pe:compiled -> file:bytes:mime:pe:compiled** from the context menu:



Question 7: How many files share that same compile time?

Filtering Results in Synapse

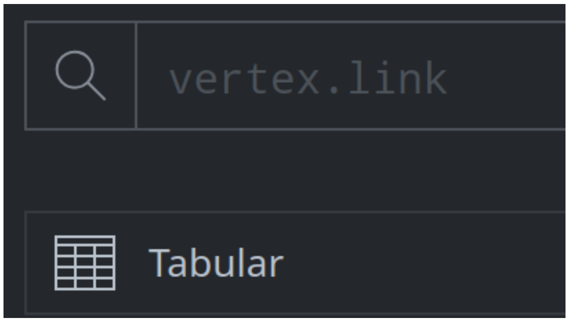
Exercise 2

Objectives:

- **Use the column filters to display a subset of your results.**

You are researching a malicious IPv4 address and want to identify any potential malware that communicates with the IP.

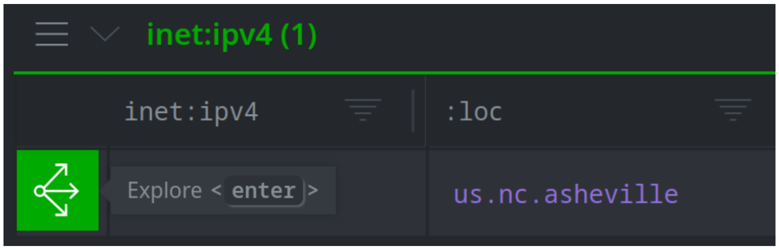
- In the **Research Tool,** ensure your **Storm Query Bar** is in **Lookup mode** and your display mode is set to **Tabular:**



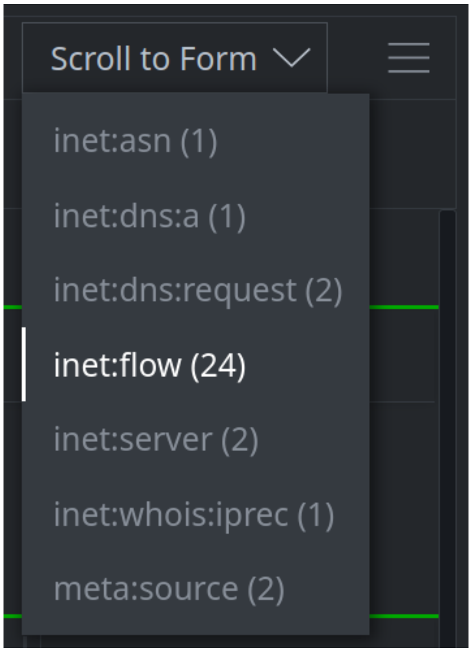
- Enter the following in the **Storm Query Bar** and press **Enter** to run the query:

```
31.170.167.235
```

- **Select** the node in the Results Panel. Click the **Explore** button next to the node to display adjacent nodes:



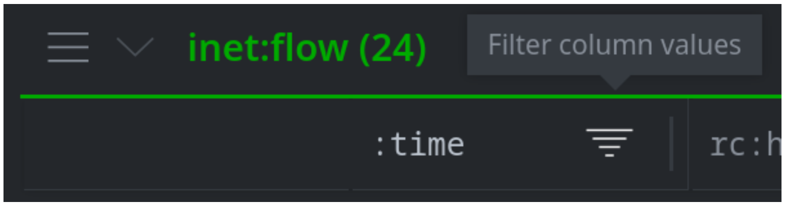
- In the **Results Panel,** locate the **inet:flow** nodes (use **Scroll to Form**) if necessary:



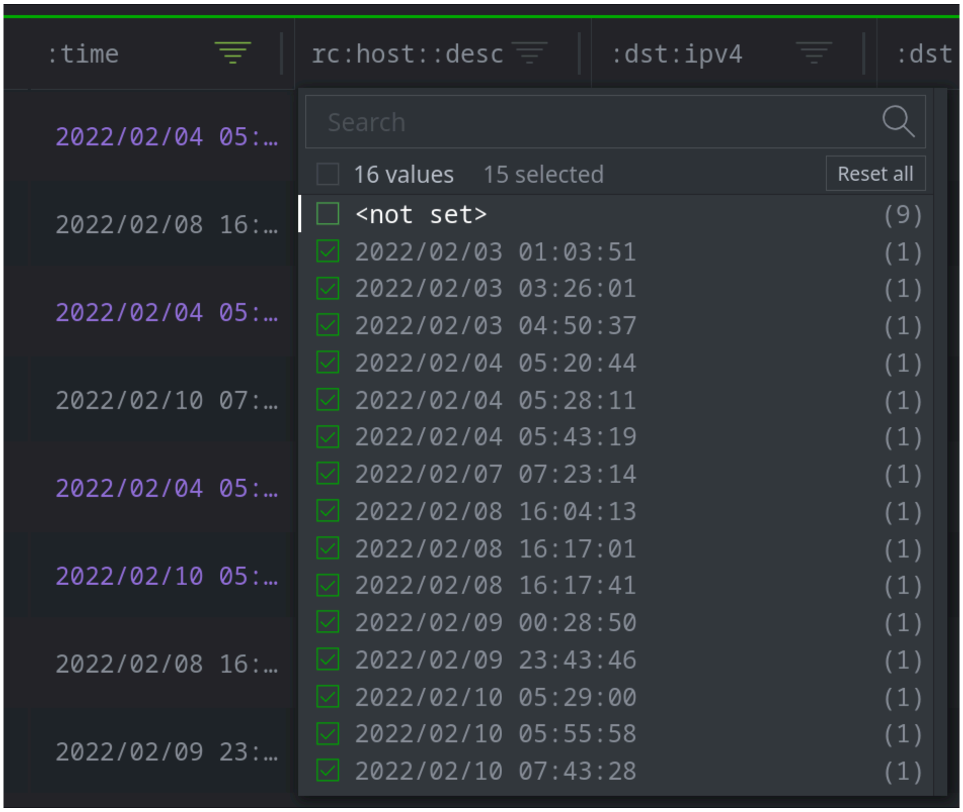
Tip: A network flow (**inet:flow**) represents a network connection between a source host (or IP) and a destination host (or IP).

Some of the results are not very useful (for example, they are missing details such as timestamps). You want to use **column filters** to focus on the data that is most helpful.

- In the **inet:flow** table, locate the **:time** column header and click the **filter icon**:



- In the filter dialog, **clear** the checkbox next to the **<not set>** entry to remove results with no **:time** value:



:time	rc:host::desc	:dst:ipv4	:dst
2022/02/04 05:…			
2022/02/08 16:…			
2022/02/04 05:…			
2022/02/10 07:…			
2022/02/04 05:…			
2022/02/10 05:…			
2022/02/08 16:…			
2022/02/09 23:…			

Search

□ 16 values 15 selected Reset all

```
□ <not set>               (9)
☑ 2022/02/03 01:03:51     (1)
☑ 2022/02/03 03:26:01     (1)
☑ 2022/02/03 04:50:37     (1)
☑ 2022/02/04 05:20:44     (1)
☑ 2022/02/04 05:28:11     (1)
☑ 2022/02/04 05:43:19     (1)
☑ 2022/02/07 07:23:14     (1)
☑ 2022/02/08 16:04:13     (1)
☑ 2022/02/08 16:17:01     (1)
☑ 2022/02/08 16:17:41     (1)
☑ 2022/02/09 00:28:50     (1)
☑ 2022/02/09 23:43:46     (1)
☑ 2022/02/10 05:29:00     (1)
☑ 2022/02/10 05:55:58     (1)
☑ 2022/02/10 07:43:28     (1)
```

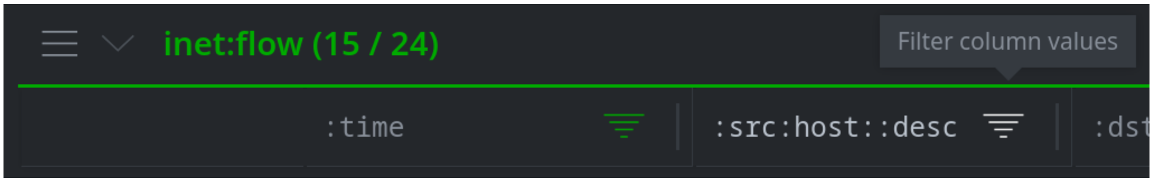
- **Click** anywhere outside the filter dialog to close the dialog.

  Question 1: How many results are present after applying the filter?

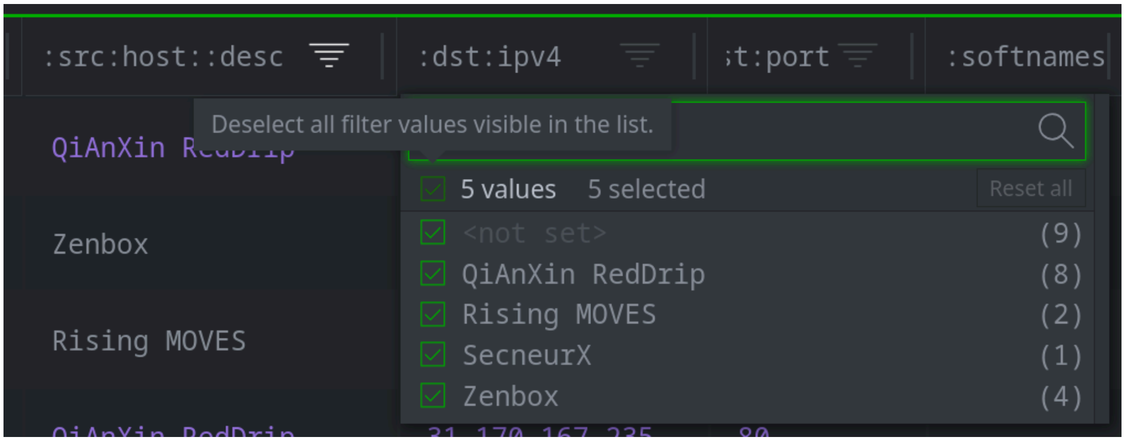
The **:src:host::desc** column indicates that these network flows came from a malware sandbox service (the descriptions are the names of vendor sandboxes).

You want to look at the results that came from vendor QiAnXin.

- In the **inet:flow** table, locate the **:src:host::desc** column header and click the **filter icon**:



- **Clear** the checkbox next to **5 values** to **remove** all selections:



:src:host::desc | :dst:ipv4 | ;t:port | :softnames

Deselect all filter values visible in the list.

QiAnXin RedDrip

Zenbox

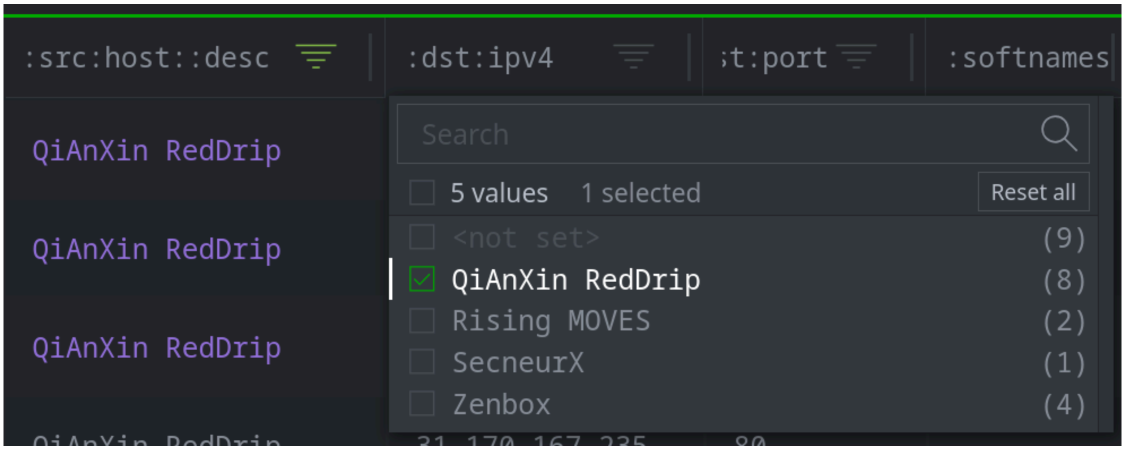
Rising MOVES

☑ 5 values 5 selected Reset all

☑ <not set> (9)
☑ QiAnXin RedDrip (8)
☑ Rising MOVES (2)
☑ SecneurX (1)
☑ Zenbox (4)

This will temporarily **hide** all of the results because you deselected (filtered out) all values.

- **Select** the checkbox next to **QiAnXin RedDrip**:



:src:host::desc | :dst:ipv4 | ;t:port | :softnames

QiAnXin RedDrip

QiAnXin RedDrip

QiAnXin RedDrip

Search

□ 5 values 1 selected Reset all

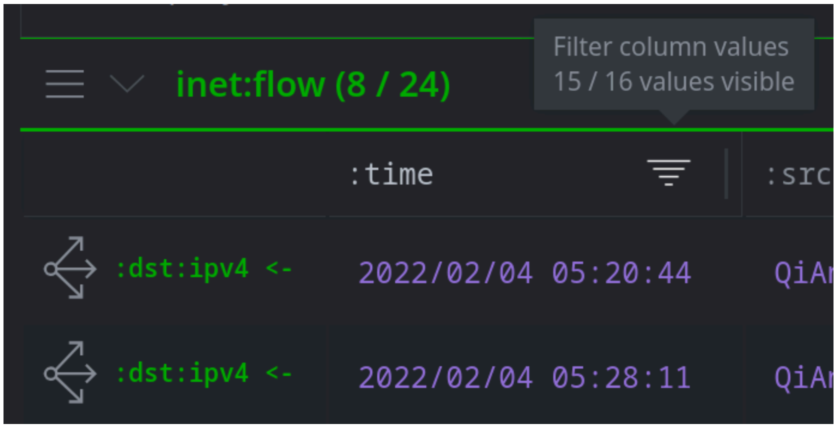
□ <not set> (9)
☑ QiAnXin RedDrip (8)
□ Rising MOVES (2)
□ SecneurX (1)
□ Zenbox (4)

- **Click** anywhere outside the filter dialog to close the dialog.

Question 2: How many results are present after applying the filter?

From here, you could query the nodes, continue to Explore, etc. For now we will reset our filters so they do not affect other queries.

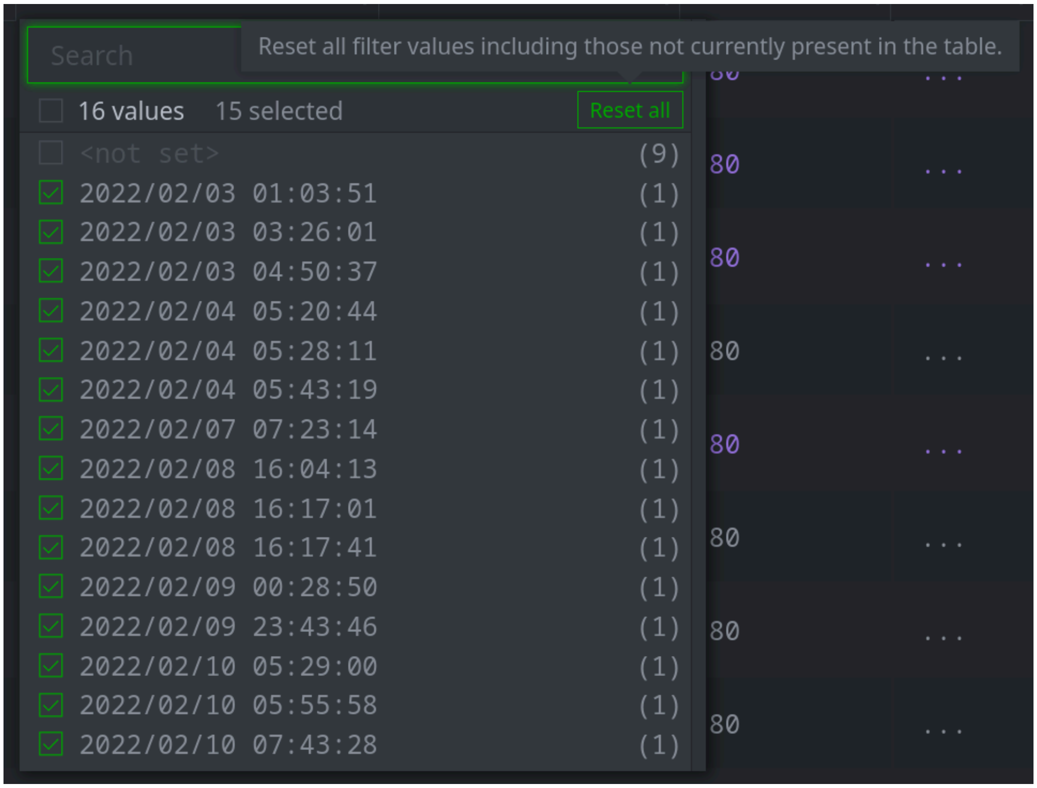
- **Click** the filter icon on the **:time** header:



:dst:ipv4 <- 2022/02/04 05:20:44 QiA

:dst:ipv4 <- 2022/02/04 05:28:11 QiA

- **Click** the **Reset all** button to remove all filters:


Search
Reset all filter values including those not currently present in the table.
Reset all

□ 16 values 15 selected

□	<not set>	(9)
☑	2022/02/03 01:03:51	(1)
☑	2022/02/03 03:26:01	(1)
☑	2022/02/03 04:50:37	(1)
☑	2022/02/04 05:20:44	(1)
☑	2022/02/04 05:28:11	(1)
☑	2022/02/04 05:43:19	(1)
☑	2022/02/07 07:23:14	(1)
☑	2022/02/08 16:04:13	(1)
☑	2022/02/08 16:17:01	(1)
☑	2022/02/08 16:17:41	(1)
☑	2022/02/09 00:28:50	(1)
☑	2022/02/09 23:43:46	(1)
☑	2022/02/10 05:29:00	(1)
☑	2022/02/10 05:55:58	(1)
☑	2022/02/10 07:43:28	(1)

- **Click** anywhere outside the filter dialog to close it.
- **Repeat** these steps to **remove all filters** from the **:src:host::desc** column.

Filtering Data in Synapse

Exercise 3

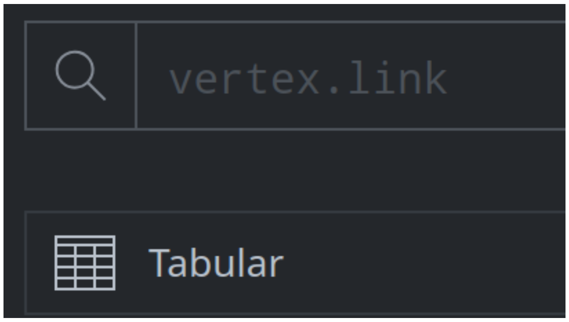
Objectives:

- **Use the 'query' menu to filter your results by running a Storm query.**

Part 1

You are researching the APT1 FQDN `earthsolution.org` and want to find any malware that queries this domain or any of its subdomains.

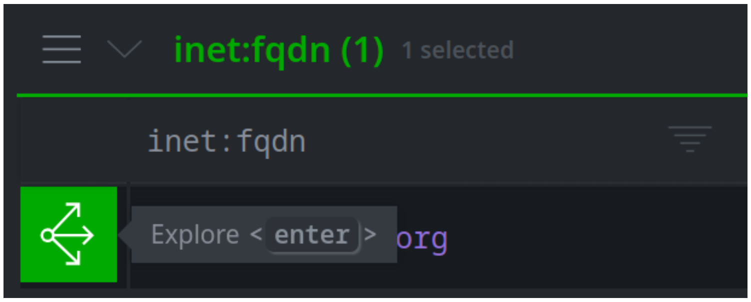
- In the **Research Tool,** ensure your **Storm Query Bar** is in **Lookup mode** and your display mode is set to **Tabular:**



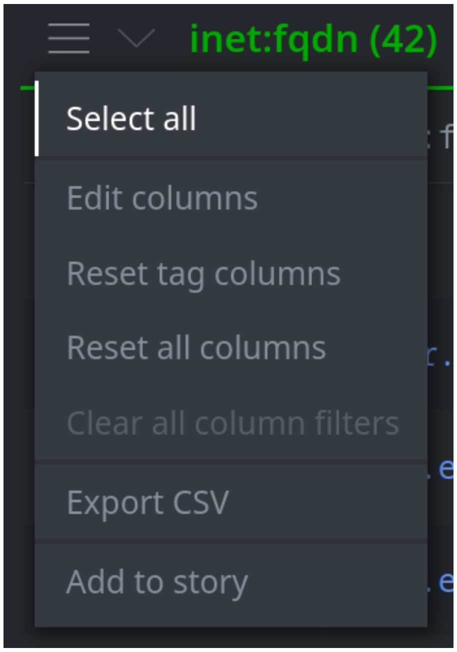
- Enter the following in the **Storm Query Bar** and press **Enter** to run the query:

```
earthsolution.org
```

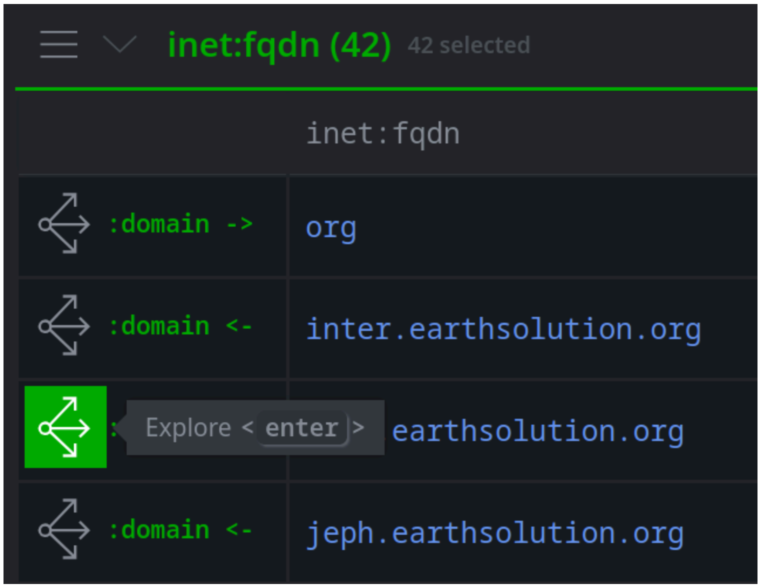
- **Select** the node in the Results Panel. Click the **Explore** button next to the node to display adjacent nodes:



- Click the **hamburger menu** to the left of the **inet:fqdn** header and choose **Select all** to select all of the **`inet:fqdn`** nodes:

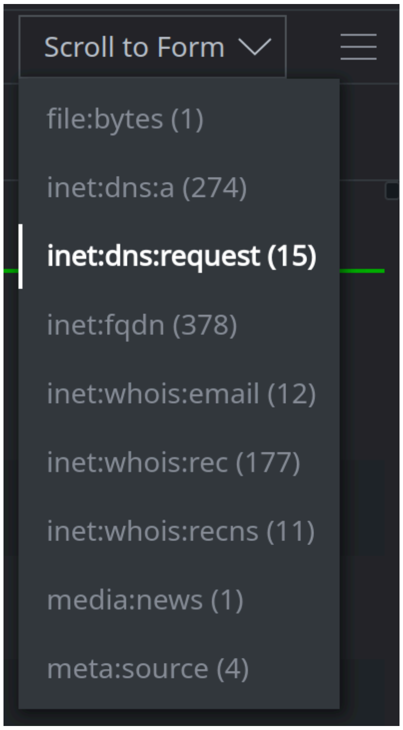


- Click the **Explore** button next to any selected FQDN to display adjacent nodes:

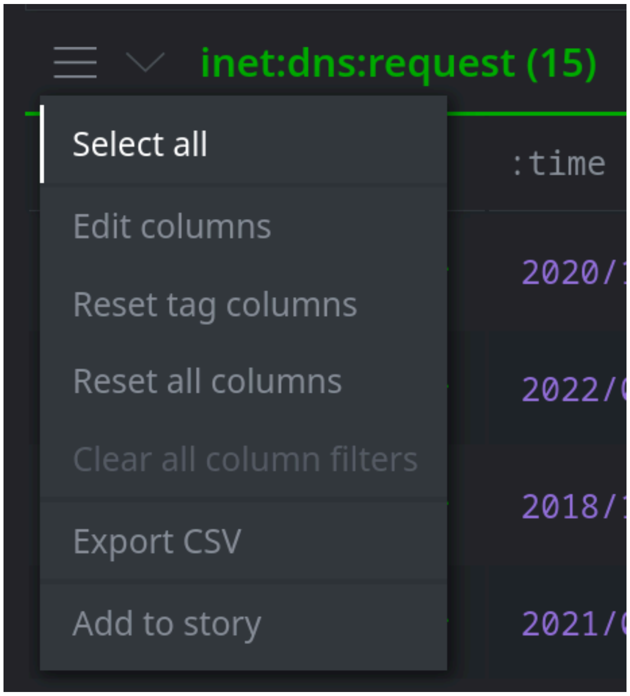


	inet:fqdn
:domain ->	org
:domain <-	inter.earthsolution.org
:	earthsolution.org
:domain <-	jeph.earthsolution.org

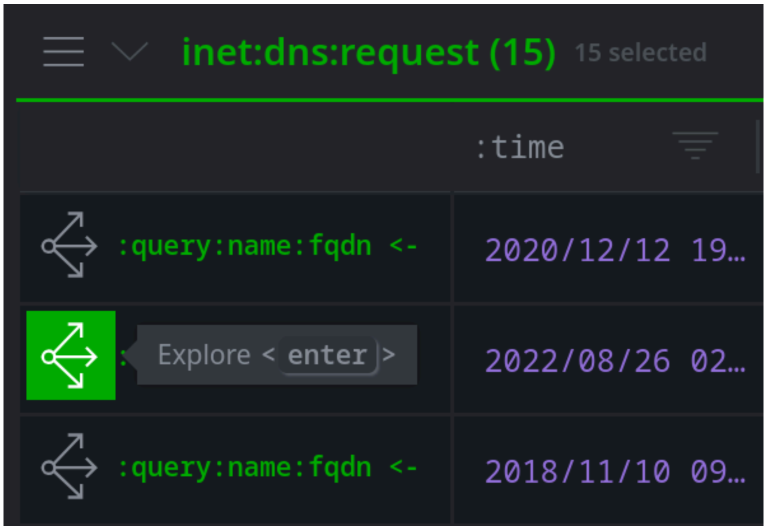
- Click the **Scroll to Form** button and choose `inet:dns:request` from the dropdown menu:



- Click the **hamburger menu** to the left of the `inet:dns:request` header and choose **Select All**:



- Click the **Explore** button next to any DNS request to display adjacent nodes:

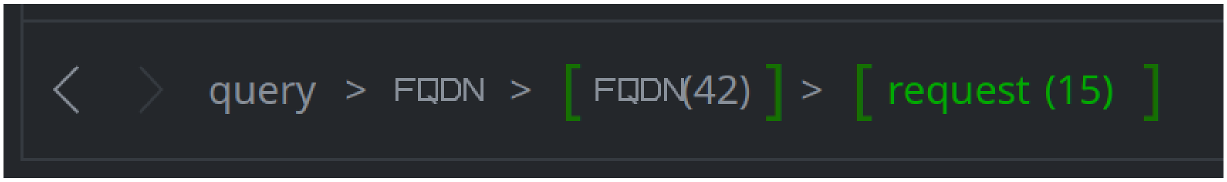


Question 1: How many files query FQDNs associated with **`earthsolution.org`?**

Question 2: Which FQDNs do the files query?

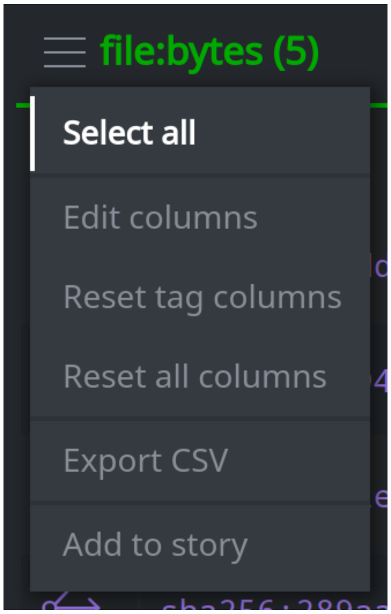
Part 2

We want to continue researching these files, but our breadcrumb trail is getting long:

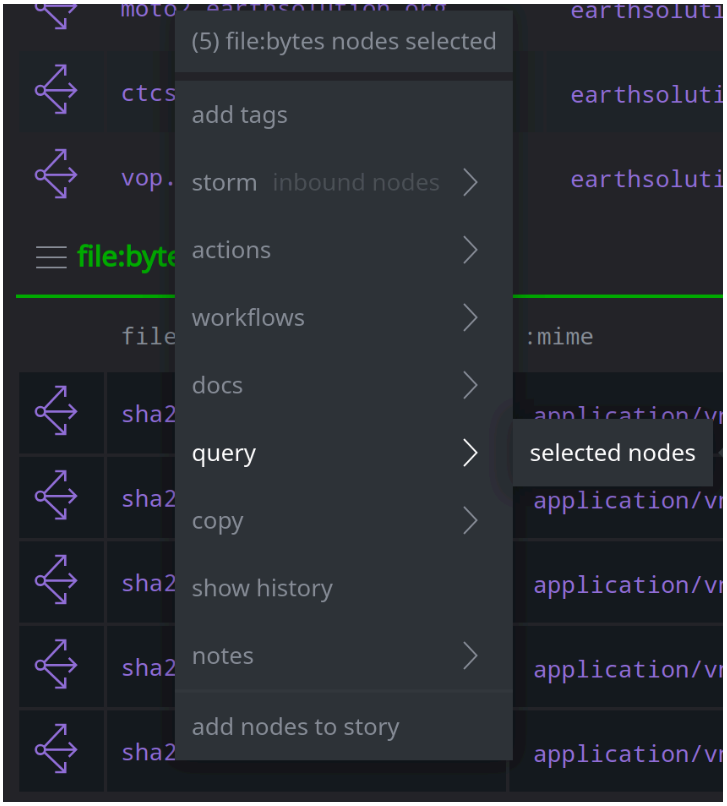


We will filter from our current results and start a new Storm query using just the files.

- Click the **hamburger menu** to the left of the **`file:bytes`** header and choose **Select All**:



- **Right-click** any of the selected files and choose **query > selected nodes**:



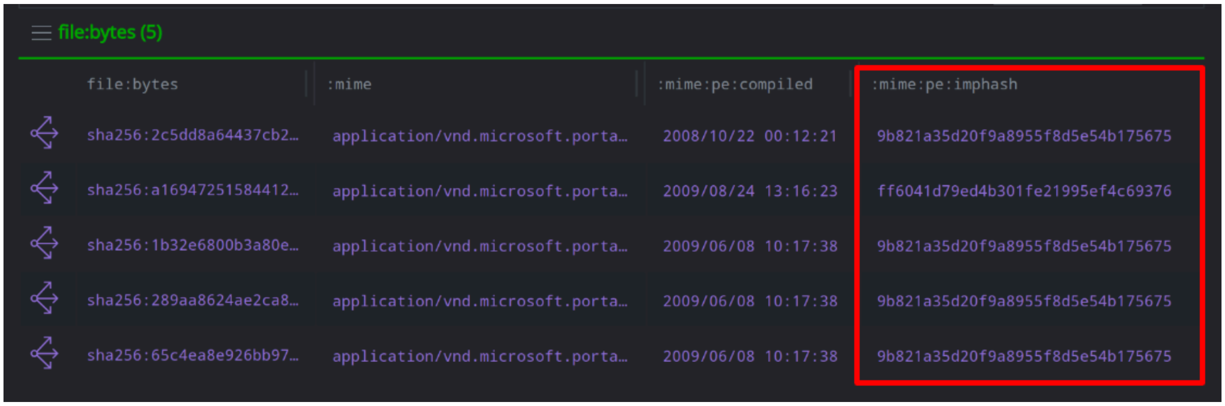
Question 3: What Storm query does Synapse enter into the Storm Query Bar after selecting the **query** option?

Question 4: What happened to your breadcrumbs after selecting this option?

Question 5: What nodes are visible in your Results Panel after selecting this option?

Part 3

You notice that **four** files in your results have the same PE import hash (imphash) value (`:mime:pe:imphash`):



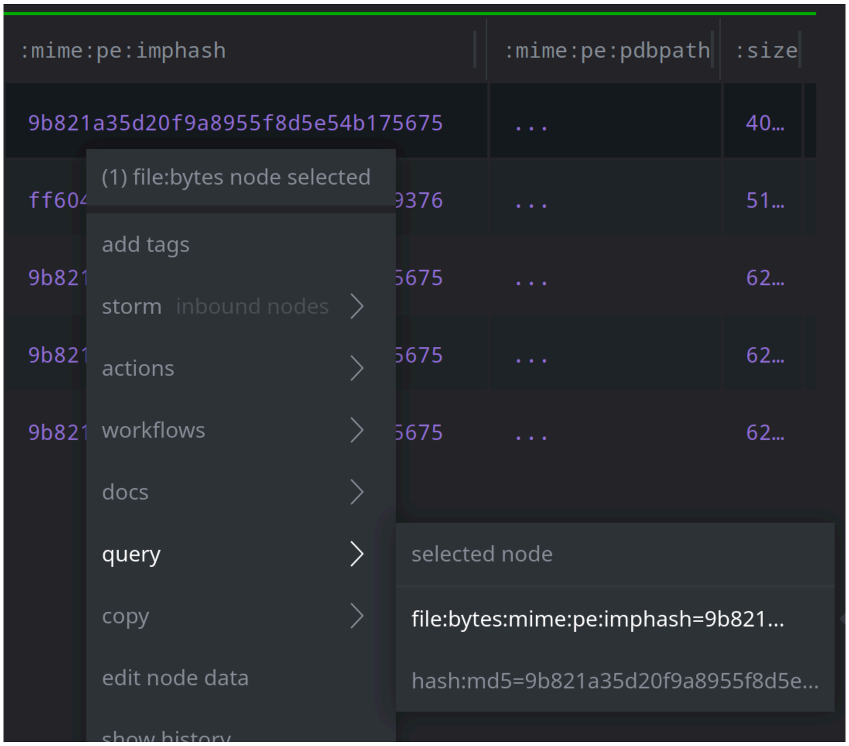
file:bytes (5)

	file:bytes	:mime	:mime:pe:compiled	:mime:pe:imphash
	sha256:2c5dd8a64437cb2…	application/vnd.microsoft.porta…	2008/10/22 00:12:21	9b821a35d20f9a8955f8d5e54b175675
	sha256:a16947251584412…	application/vnd.microsoft.porta…	2009/08/24 13:16:23	ff6041d79ed4b301fe21995ef4c69376
	sha256:1b32e6800b3a80e…	application/vnd.microsoft.porta…	2009/06/08 10:17:38	9b821a35d20f9a8955f8d5e54b175675
	sha256:289aa8624ae2ca8…	application/vnd.microsoft.porta…	2009/06/08 10:17:38	9b821a35d20f9a8955f8d5e54b175675
	sha256:65c4ea8e926bb97…	application/vnd.microsoft.porta…	2009/06/08 10:17:38	9b821a35d20f9a8955f8d5e54b175675

You want to look for additional files that have the same import hash[1].

- Right click the **:mime:pe:imphash** column for any file where the import hash value is **`9b821a35d20f9a8955f8d5e54b175675.`** Select **query > file:bytes:mime:pe:imphash=9b821…** :

[1] An **import hash** is an MD5 hash of the functions imported by a PE executable file. Files with the same import hash value use the same imported functions in the same order. This may help identify similar files (in this case, related malware samples) that were compiled from the same or similar source code.



:mime:pe:imphash	:mime:pe:pdbpath	:size
9b821a35d20f9a8955f8d5e54b175675	...	40…
ff604 9376	...	51…
9b821 5675	...	62…
9b821 5675	...	62…
9b821 5675	...	62…

(1) file:bytes node selected
add tags
storm inbound nodes
actions
workflows
docs
query
copy
edit node data
show history
selected node
file:bytes:mime:pe:imphash=9b821...
hash:md5=9b821a35d20f9a8955f8d5e...

Question 6: What does Synapse enter into your Storm Query Bar after selecting the **query** option?

Question 7: How many files are returned when you run this query?